2600

APRIL, 1985

VOLUME TWO, NUMBER FOUR

what a white box can do

This article describes how to take a standard touch tone keypad and convert it to a portable unit. This information is essentially public domain and was originally downloaded from the old OSUNY BBS. It is also available on Sherwood Forest II and undoubtedly other BBS's around the world. It is being reprinted and explained here for those who are not able to get this type of information from BBS's and for those who are just starting out in the phone phreak business.

If you convert a touch tone keypad in the manner described below, you will become more familiar with the inner workings of your telephone and telephone system. You will also be able to use rotary phones to call extenders or phone services that respond to touch tones, because now you will be able to generate touch tones yourself without having to depend on the phone. You will also be able to use payphones that turn off their touch tones after you dial your number. In addition, there are often phones in airports, hotels, and at bank machines which have no dial on them and automatically dial a pre-programmed number (usually a service number), which can be used by someone with a portable dialer to enter a number or numbers before the pre-programmed one starts to dial, thus gaining control or causing a wrong number. It is often the case that after the number dials or the error message ends, the phone might eventually revert to a dial tone which can be used. A portable tone generator like this is more useful than tapping the plunger on the telephone when no dial or keypad are available, which takes patience and effort. If you purchased a portable dialer, it would cost from $20 to $30 dollars. Good ones that remember 99 numbers, are password protected, and are smaller than a calculator cost $60 to $70 dollars. Often they are available from long distance services for less, when you sign up for them. The procedure related below is a nice way to bring new life to an old touch tone phone or keypad. Please note that the building and the general use of this device is legal and fun.

First of all, the tones made by a touch tone telephone are not single tones, they are a combination of two tones, making "DTMF" (dual tone multi-frequency). The normal tone telephone dials 12 different signals, but is capable of dialing 16 different signals.

The power required by a wired keypad is about 25 volts, but they will work with as little as 15, thereby allowing you to use two 9 volt radio batteries. As you may have guessed, they are also designed to operate with a telephone type speaker (and phone line), and not the standard 8 ohm speaker which needs to be used for adequate volume. To accomplish this, we use a matching transformer, this is one of those miniature ones available at Radio Shack. Enough of the theory, now for the circuit.

You will need:
- A touch tone keypad
- A miniature 1000 to 8 ohm transformer (Radio Shack # 273-1380)
- A standard 8-ohm speaker
- Two 9-volt radio batteries
- Two 9-volt battery clips
- A case to put it all in (optional)

A few construction notes. It is suggested that you solder and tape all connections. It is also important to read this entire article before attempting to construct this.

First, connect the RED wire of the transformer to either terminal on the speaker. Now connect the WHITE wire from the transformer to the other terminal on the speaker. Next, connect the RED (positive) wire of one battery clip to the black wire of the other battery clip. Now connect the remaining RED wire on the second battery clip to the GREEN wire from the touch tone pad. Connect the BLUE wire from the touch tone pad to the ORANGE-and-BLACK striped wire from the touch tone pad. To these two wires, now connect the remaining black lead from first battery clip. You have now finished the power connection to the keypad. Connect the BLACK wire from the keypad to the BLUE wire on the transformer. Next connect the RED-and-GREEN striped wire from the keypad to the GREEN wire on the transformer. The BLACK wire on the transformer should not be connected to anything, along with quite a few wires from the keypad. The connection of the keypad is now complete. All you have to do is connect two nine volt batteries to the battery clips, and you'll be ready to go. You may want to mount it in a case for easy portability. Note that the silver box modification CAN be made to this unit, allowing complete remote phreaking. This is a bit more complex than the conversion you have accomplished above. When none of the buttons are pressed, this unit uses NO power, thereby eliminating the need for a power switch, and extending the life of the batteries.

a phone phreak scores

This is another story to add to the annals of social engineering, one which we all can learn from...

A few months ago my Mom had some people refinish and blacktop our driveway. So she called some companies in the phone book, and she chose the cheapest one. They came and did most of the work, and Mom paid them, providing they came back soon to finish the blacktopping job. This all sounded fine, but after several weeks of the company calling up and postponing the final work, Mom wanted it done. She decided to visit the company at the address listed in the phone book, because she would always get an answering machine when she called them, but when she got there, she found out that it was just the back room of a storefront and that the company had vacated it a few months earlier. When she tried calling them their number had been changed. So I did a CNA on their new number for Mom, and she visited the new address that I got. When Mom got to the new address she found a vacant lot. It was at this point that it started to sound pretty fishy to Mom and I. But how could we find out where they were, if they gave a fake address to the phone company?

That's when it occurred to me to call the business office that handles that company's telephone. I called and they answered: "Your number, please." So I gave them the company's number, and I proceeded to tell them how I did not get my last phone bill, and how I wanted to make sure they were sending it to the right address. They told me the real name and address (not the one at CNA or Directory Assistance, which was the one it was listed under, there is a difference, you know), they asked if I was "Mr. So and So," to which I responded "Yes." Then they asked if I wanted to change the mailing address. I said, "No, that's my partner's address. No need to change it. Thank you."

And that was it. I found their address. Mom visited their new location, which happened to be a trailer in the middle of a big field with a telephone and a power cable going into it. When she found the people at the company, they were quite startled, because it seemed that they did not have a license to do the work that they were doing and had several other customers and some government agencies looking for them. Since Mom had the goods on them, they were obliged to finish our driveway, and that's all Mom wanted after all.

HACKING PACKARD by Bioc Agent 003

PREFACE

The purpose of this tutorial is to give potential hackers useful information about Hewlett-Packard's HP2000 systems. The following notation will be used throughout this tutorial:

<CR> - carriage return, RETURN, ENTER, etc.
^C - a control character (control-C in example)
CAPITAL LETTERS - computer output & user input

SYSTEM INFORMATION

Each HP2000 system can support up to 32 users in a Timeshared BASIC (TSB) environment. The systems usually run a version of Hewlett Packard's Timeshared/BASIC 2000 (various Levels).

LOGON PROCEDURE

Once connected to a HP2000, type a numeral followed by a <CR>. The system should then respond with: PLEASE LOG IN. If it does not immediately respond, keep on trying this procedure until it does (they tend to be slow to respond).

User ID: The user id consists of a letter followed by 3 digits, eg. H241.

Password: The passwords are from 1 to 6 printing and/or non-printing (control) characters. The following characters will NOT be found in any passwords so don't bother trying them: line delete (^X), null (^@), return (^M), line feed (^J), X-OFF (^S), rubout, comma (^L), space (^'), back arrow (<-), & underscore ( ). HP also suggests that ^E is not used in passwords (but I have seen it done!).

The logon format is: HELLO-A123,PASSWD Where: HELLO is the login command. It may be abbreviated to HEL. A123 is the user id & PASSWD is the password.

The system will respond with either ILLEGAL FORMAT or ILLEGAL ACCESS depending upon whether you screwed up the syntax or it is an invalid user id or password. The messages: PLEASE LOG IN, ILLEGAL FORMAT, & ILLEGAL ACCESS also help you identify HP2000 systems.

The system may also respond with ALL PORTS ARE BUSY NOW - PLEASE TRY AGAIN LATER or a similar message. One other possibility is NO TIME LEFT which means that they have used up their time limit without paying.

Unlike other systems where you have a certain amount of tries to login, the HP2000 system gives you a certain time limit to logon before it dumps you. The system default is 120 seconds (2 minutes). The sysop can change it to be anywhere between 1 and 255 seconds, though. In my experience, 120 seconds is sufficient time for trying between 20-30 logon attempts while hand-hacking & a much higher amount when using a hacking program.

USERS

The various users are identified by their user id (A123) & password. Users are also identified by their group. Each group consists of 100 users. For example, A000 through A099 is a group, A100 through A199 is another group, & Z900 through Z999 is the last possible group. The first user id in each group is designated as the Group Master & he has certain privileges. For example, A000, A100,...H200..., & Z900 are all Group Masters. The user id A000 is known as the System Master & he has the most privileges (besides the hardwired sysop terminal). The library associated with user Z999 can be used to store a HELLO program which is executed each time someone logs on.

So, the best thing to hack on an HP2000 system is the System Master (A000) account. It is also the only user id that MUST be on the system. He logs on by typing: HEL-A000,PASSWD. You just have to hack out his password. If you decide to hack Z999, you can create or change the HELLO program to give every user your own personal message every time he logs on! This is about all you can do with Z999 though since it is otherwise a non-privileged account.

LIBRARY ORGANIZATION

Each user has access to 3 levels of libraries: his own private library, a group library, and the system library. To see what is in these libraries you would type: CATalog, GROup, & LIBrary respectively (all commands can be abbreviated to the first 3 letters). The individual user is responsible for his own library and maintaining all the files. If a program is in your CATALOG, then you can change it.

[Group Masters]

Group Masters (GM) are responsible for controlling all programs in the Group libraries. Only members of the group can use these programs. These are viewed by typing GROUP. For example, user S500 controls all programs in the Group library of all users beginning with id S5xx. Other users in the group CANNOT modify these programs. All programs in the group library are also in the Group Masters private library (CATALOG), therefore he can modify them! The Group Master also has access to 2 privileged commands. They are: PROtect & UNProtect. With PROTECT, the Group Master can render a program so it cannot be LISTed, SAVed, CSAved, PUNched to paper tape, or XPUnched. For example, if the GM typed PRO-WUMPUS, other users in the group would be able to RUN WUMPUS but they would not be able to list it. The GM can remove these restrictions with the UNProtect command.

[System Master]

There is exactly one System Master (SM) and his user id is A000. He can PROTECT & UNPROTECT programs in the System Library.

All users have access to these files by typing LIBRARY to view them. Only the System Master can modify these files since his private library & group library constitute the System Library. The SM also has access to other privileged commands such as: DIRECTORY: this command will printout all files and programs stored on the system according to users. DIR will print out the entire directory. DIR-S500 will start listing the directory with user S500. Example:

```
   DIR
      BOCES ED 1   053/84   1243
    ID     NAME    DATE      LENGTH    DISC       DRUM
   A000   ALPHA   043/84     00498   001384
          BCKGMN  053/84     04564   001526
          FPRINT  053/84     00567   002077
          STOCK   035/84     04332   002753
          TFILE   020/83 F   00028   002804
          WUMPUS  053/84  P  02636   003142
   B451   BLJACK  316/75     03988   011887
          GOLF    316/75     02773   011911
   S500   GIS     050/84 C   03120   019061
          GISCL4  050/84 F   03741   022299
   Z999   HELLO   021/84     00058   011863
```

In this example, the system name is BOCES ED 1. The date of the printout is the 53rd day of 1984 (053/84) and the time is 12:43 (24-hr). The files appearing under A000 are those in the System Library. The DATE associated with the program is the date it was last referenced. The LENGTH is how long it is in words. DISC refers to its storage block location on one of the hard drives. DRUM refers to its location on the drum storage unit. Only sanctified programs are stored on a drum to increase their access time. The letters after the date refer to F if it is a file, P means it is protected, and C means the program is compiled. In the example the system program, WUMPUS, was last used on the 53rd day of 1984 (2-22-84); it is currently unlistable (PROtected) and it occupies 2636 words of memory starting at disc block 3142. The command SDIrectory will print out programs that are only stored on drum. Most system directories are usually longer than the example. The above example is an abridged version of a 43 page directory! The <BREAK> key will STOP the listing if necessary.

REPORT

The REPORT command will show the USER id, how much terminal TIME they have used since the last billing period (in minutes), and how much disc SPACE they are using. Example:

```
   REPORT
       BOCES ED 1 055/84    1905
    ID   TIME  SPACE      ID   TIME  SPACE       ID   TIME  SPACE
   A000 01150 12625     B451 00003 05861      B864 00000 00000
   S500 00239 06861     S543 00421 00000      Z999 00000 00058
```

The advantage of hacking the A000 password first is that you can use the privileged commands to see which user id's exist and what programs are stored where so that you can further penetrate the system.

NOTE: There are different levels (versions) of TSB/2000. This article is based primarily on Level F. Most of the levels are similar in their commands so the differences should not affect the hacker. Also, some systems are customized. Eg, one system I know doesn't have the MESSAGE command because they don't want the operator bothered with messages. Another system says ??? instead of PLEASE LOG IN and ILLEGAL instead of ILLEGAL ACCESS. These are only trivial problems, though.

PROGRAMS

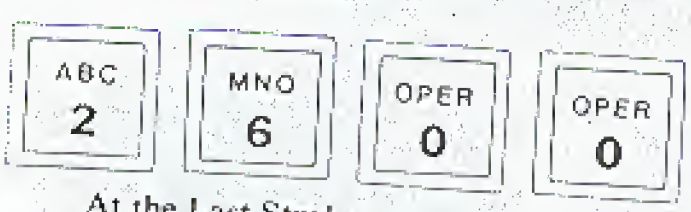
Hewlett-Packard often supplies programs from their TSB Library for the systems. Utilities such as ASCII$, FPRINT, & others are almost inevitably found on every system. Standard games such as WUMPUS, STOCK, LUNAR, & many others are also a "system must." Other companies offer very large programs for the HP2000 also. GIS (Guidance Information Systems) is a database to help guidance counselors help students to select colleges, jobs, financial aid, etc. GIS is usually found in the S5xx group library (anyone with an S5xx password can use it). Unfortunately, sometimes these programs are set so that a certain password will automatically RUN them. In some cases you can abort by pressing the <BREAK> key. There is a BASIC function [X=BRK(0)] that disables the <BREAK> key. In this case, only the Sysop or the program can throw you into BASIC.

There are many alleged bugs on the HP2000 that allow users to do all sorts of things. If you run across any of these be sure to let us know.

Most of the HP2000 systems are used by schools, school districts, BOCES, and various businesses. This was an ideal system for schools before micro- computers existed. The HP2000 system has been in existence since around 1973. It has been replaced by the HP3000 but there are still many HP2000 systems in existence & I believe that they will stay there for awhile.

Here are the dial-ups to a few HP2000 systems to get you started: [203/622-1933], [212/777-7600]#, [312/398-8170], [314/645-1289], [914/327-5540]

- This # belongs to NYU. Type 'HP' at the prompt. Then hit the <BREAK> key slowly until you see the backslash (\) prompt. You are then in.



FLASH FLASH

At the Last Stroke...

Associated Press

At precisely 11 am on April 2nd a man's voice was heard on Britain's telephone talking clock for the first time.

The smooth baritone voice of part-time actor Brian Cobby, 55 years old, replaced the modulated contralto of Pat Simmons, whose voice was retired after 21 years at precisely 10:59 and 30 seconds.

Last December Mr. Cobby was chosen from among 5,000 competitors to tell the nation the precise time every 10 seconds in a recorded telephone message that is expected to receive 300 million calls this year.

Only two other voices have been heard on the telephone clock since it was devised in 1930. Both were women's.

Mr. Cobby, an assistant supervisor at a telephone exchange in Brighton in southern England, said it was "a great honor to be Britannia's wristwatch." He was paid the equivalent of $6,000 to record the 8,640 time announcements in one 24-hour period.

Good Apples for the Soviets

The New York Times

The Reagan Administration appears to be prepared to cooperate with Soviet efforts to put personal computers in secondary schools, according to industry officials negotiating export licenses.

"We expected it would be more difficult, so I was quite pleasantly surprised," said Albert Eisenstadt, a vice president of Apple Computer who was in Washington to discuss computer exports with Commerce and Defense Department officials. "They just want to make sure we do it right."

The Soviets are already producing their own "Agat"—a Soviet knockoff of an Apple II, but they are not able to produce enough. That is why IBM, Commodore, Sinclair Research Ltd., and Apple are all competing for the Soviet market.

The Commerce Department has argued that it makes no sense to bar American companies from selling computers the Russians could easily obtain in Japan and Britain. The Defense Department, which has taken a harder line, seems unperturbed by the thought of exporting thousands of machines, provided they are used for education. By law the sale of "hardened" machines that are designed to withstand battlefield conditions are barred.

Hackers Go Free

The New York Times

Four teenagers who used home computers to tap into a space agency computer at the Marshall Space Flight Center will not be prosecuted, United States Attorney Frank Donaldson announced.

The FBI seized the youths' computer equipment at their homes in Huntsville, Alabama, last July 16 after tracing the phone calls used to enter the computer. Unauthorized access to a computer is not permitted.

One of the youths, Robert Grumbles, 17 years old, said he wished the FBI would return his $5,000 computer because "I don't see any reason for them to keep it." [Keep up the spirit, Rob.]

Robot Kills Man

The New York Times

Last summer, a Michigan man was the first worker killed by a robot in this country. The 34-year-old victim, working with automated die-casting machinery last July, was pinned between the back of a robot and a steel pole, the National Center for Disease Control reported. The worker suffered a heart attack, lapsed into a coma and died five days later.

There are more than 6,200 robots in use nationwide.

'Santa Fraud'

Associated Press

Randy Grimm didn't know it cost 55 cents every time he called a sports trivia game, so the 15-year-old dialed it 330 times last month hoping to answer the quiz correctly and win a prize. His mother received her telephone bill: 18 pages long, with more than $100 worth of "976" calls. But Ms. Grimm doesn't want to pay, and neither do the parents of Josie Aaronson-Gelb and Rachel Krebs-Falk, who repeatedly called a Santa Claus message last December, not knowing it was costing 50 cents a shot.

Jessica and Rachel, both 7, are plaintiffs of record in a $10 million lawsuit filed in San Francisco Superior Court against Pacific Bell and the company that operates the Santa Claus Line.

The suit accuses Bell and "Santa Fraud" of deceptive advertising "designed to falsely mislead children into believing the calls were free" and inducing them to call repeatedly.

The suit, filed on behalf of all California children, asks for a refund for an estimated 100,000 families and $10 million in punitive damages to set up a children's protection fund to fight deceptive advertising.

Overseas Pirates

Inter Press Service

In the large cities in Holland last year, you couldn't switch on the TV at times without tuning in to a pirate station. With equipment costing as little as 20£, they would break into the cable networks that service as much as 90% of Holland's urban areas. Some would transmit anything they could get their hands on, just for the sport of it—while others tried to do things that were genuinely new to TV. Artists and performers were quick to join in, and for a while the country enjoyed a madcap, unpredictable after-hours TV service. There was everything from pop video to pornography, from foreign TV shows to feature films, even one station that transmitted occasional satanic sermons.

Threats of prosecution over copyright of some of the hoarded material put a stop to many of the pirates. In addition, the cable owners have now started switching off their systems outside regular hours, a remedy that was deemed illegal on a technicality last year. Most of the pirates have now gone back to the radio and the anarchic highlights of after-hours Dutch cable TV may never be seen again.

Real Life War Games?

Time

A Stanford University computer operations specialist has filed a lawsuit to block the U.S. from hooking up a computer system that would automatically launch nuclear missiles in response to an incoming nuclear attack.

Clifford Johnson argues that it is unconstitutional to give war-making power to the so-called launch-on-warning computer system. He recently suffered a legal setback when the federal district judge declined to render a decision. The case will now go to the U.S. Court of Appeals in San Francisco.

Although the U.S. does not officially have the capability to deploy the launch-on-warning system, the technology to do so is definitely being developed by the Pentagon, Johnson claims. And he says, Secretary of Defense Caspar Weinberger, who is the defendant in the lawsuit, has stated that the U.S. has not closed the door on the launch-on-warning option.

Not only does Johnson fear that the launch-on-warning computer could somehow malfunction and start a nuclear war, but he points out that the satellites and radar that would warn the computer of an enemy missile launch could themselves sound a false alert, one that the computer would be unable to distinguish from the real thing.

"To hook this system up in peacetime is in essence a act of war," Johnson says, "because there is a definite risk of it going off accidentally."

Silver Pages

Courtland Bloch Reports

Southwestern Bell Media is publishing a new phone book, printed in a larger typeface for senior citizens. It is expected to arrive in New Jersey in August and will be published in 110 cities across the United States and will feature stores that offer discounts to those age 60 and older. The directory, called the Silver Pages, will also include information on agencies on aging. [Hopefully, these directories won't weigh 50 pounds.]

Other News

Courtland Bloch Reports

- A telephone operators' union threatened to picket an appearance by Joan Rivers at an AFL-CIO meeting. The union thinks that the comedian went a bit too far in bad-mouthing operators in a commercial she did for MCI Communications, which doesn't use operators. The 650,000-member Communications Workers of America also charges that Rivers reneged on her acceptance of a challenge to work a day as an operator.
- The telephone company cannot seem to get the lines uncrossed at Pleasantville International. The company has six telephone lines. For the last several weeks, incoming callers have been cutting into conversations in progress on other Pleasantville lines. And when calls route it, all lights flash on all the phones, so it is just a guess which is the incoming call and which are calls in progress. Further, an incoming call might connect to a call-in service—one with a seductively voiced woman. "We've just been doing union business with the Christian Broadcasting Network," reported Craig MacDonald, the company's marketing director. "That's when it becomes not amusing."
- Bell Canada said it began charging large users of U.S. directory assistance to eliminate abuse of the service by customers who use free directory assistance to compile customer lists for sale to U.S. companies. Phone lines will now have free directory assistance for the first 250 requests.
- Pacific Bell has found a way to let a single phone line carry two voice and three computer conversations at the same time.
- United States banks lost an estimated $50 million to $100 million from fraudulent use of automated teller machines in 1983, with customers forfeiting millions from lost or stolen cards, the Government says. Banks swallow the bulk of the losses.

DEAR 2600:

When will it almost be impossible to use Long Distance Services? It is so easy to Phreak off them and they never catch the majority of us, but when will it stop?

Puzzled

ONLY WHEN THE WORLD IS A BURNT OUT CINDER WILL IT STOP COMPLETELY. AS TECHNOLOGY CHANGES, SO DO PHONE PHREAKS. BLUE BOXES USED TO BE THE ONLY WAY A PHREAK MADE FREE PHONE CALLS. NOW THERE ARE EXTENDERS AND ALTERNATE CARRIERS. WE DON'T THINK EXTENDERS ARE GOING TO DIE OUT ANYTIME SOON. ALTERNATE CARRIERS (SPRINT, MCI, ETC.) WILL GET HARDER TO ABUSE AS EQUAL ACCESS MOVES IN, BUT THERE WILL ALWAYS BE A WAY. WE LOVE TO HEAR ABOUT NEW METHODS.

OPEN LETTER:

7 a.m., 02/07/85: Pursuant to a telephone discussion with Reginald Dunn, head of the criminal division of the Los Angeles' City Attorney's office, I was informed that the prosecution believes it has insufficient evidence to continue the prosecution of Tom Tcimpidis, SYSOP of MOG-UR. This determination was made after I requested a review of the case on 1/11/85 after the departure of City Attorney Ira Reiner to become D.A., and while the City Attorney's office is being run by the civil service staff pending election of a new city attorney. Mr. Dunn has given me his word that the people will seek dismissal of the charges against Tom under California Penal Code Section 1385, i.e., 'Dismissal in the interests of justice.' Under California law, such a dismissal is 'with prejudice' and the people can not refile the case subsequently. To put it succinctly, a dismissal will terminate the prosecution permanently.

As [many of you] know, the City Attorney's office has previously reneged on representations made to me regarding dismissal of the charges. I wish to assure everyone that I have known Mr. Dunn for 10 years, and I trust his word completely. If he says the case will be dismissed, I am satisfied that such an action will occur.

We win, Win...win...win...win...win. My thanks to everyone who contributed to supporting Tom and me in the defense of this matter. I consider this to be a major victory for the rights of free speech over the 'big brother' machinations of the phone company.

I would be grateful if you would download this message and place it on other systems throughout the country. This is a very big victory, and the BBS and modem communities should know about it.

Again thanks for the support.

Chuck Landner, attorney for SYSOP Tom Tcimpidis.

8 p.m., 02/07/85: The case of People vs. Tcimpidis -- a.k.a. use a modem, go to jail -- was dismissed in the 'interests of justice' this morning, 2/7/85. As noted earlier, this dismissal is with prejudice, and Tom is now free of the Pacbel scourge. Another small step for something resembling justice.

Chuck

THRILLED WE ARE FOR TOM, BUT CHARGES DROPPED MEANS LAWS REMAIN. IN THIS CASE TOM GOT AWAY WITH WHAT HE DID OR THE LAW JUST REALIZED THAT THERE WAS JUST NOT ENOUGH EVIDENCE TO PROVE ANYTHING. BUT CALIFORNIA STILL HAS HORRIBLE TOUGH LAWS THAT DO NOT PERMIT PRINTING MAGAZINES LIKE 2600! YOU CANNOT EVEN DISCLOSE A PHONE NUMBER OR A PASSWORD FORMAT LET ALONE A WHOLE PASSWORD THERE. WE ARE GLAD HE GOT HIS MACHINE BACK, WHICH IS ALWAYS A PLEASANT SURPRISE. WE ENCOURAGE OUR READERS TO SPREAD THIS NEWS WHEREVER THEY GO AS IT IS A VERY IMPORTANT DEVELOPMENT. (FOR THOSE WHO DON'T KNOW, TOM TCIMPIDIS WAS THE SYSOP OF A COMPUTER BULLETIN BOARD THAT SOMEONE POSTED A CREDIT CARD NUMBER ON. THE PHONE COMPANY DECIDED TO PRESS CHARGES AGAINST HIM EVEN THOUGH HE CLAIMS NEVER TO HAVE SEEN THE NUMBER IN QUESTION. THEY TOOK HIS COMPUTER AND GOT HIM A LOT OF NATIONAL ATTENTION.)

DEAR 2600:

Have you been reading about those new high tech secure telephones? I've been thinking about what must be inside them. The closest thing I've heard to that kind of technology would be DVP - Digital Voice Processing. It's like digital audio processing, but after the voice is turned into bits, dsfdsfxscfgsjkf;ggreegfds they scramble them up and then send them off. The other side then decrypts the bits and transforms the decrypted signal back into voice. The stuff I've read (in Popular Communications Magazine, around a year ago) said that a lot of law enforcement agencies use it to scramble their radio transmissions. I believe the ones mentioned were the DEA and the Treasury police, maybe the secret service, but not, interestingly enough, the FBI?. The only problem is that it didn't work too well - many people reported hearing the agents switching the DVP off and transmitting a normal, unscrambled signal because they couldn't get it working right. However, over a land line it would probably work a lot better. And the nice thing about DVP is that it really is secure, as long as no one knows your scrambling algorithm - however, I imagine the Russians already have the plans for one of those phones, given that very few military secrets ever remain secrets for long. Besides, if the government orders several thousand of them, it stands to reason that at least one would end up in the wrong hands. Anyway, I'm not sure that knowing the innards of those phones would help you unscramble the traffic, since that might only cut down the number of possibilities to a few billion instead of a few quadrillion. The whole point of encoding something is so that your enemy does not unscramble it while the information is still useful to either of you.

I've often thought about how to do something like that with our little micros. Two people talking on the phone via a scrambled modem link have a remarkably secure connection, provided they are using the right software for mixing up the bits. I seem to remember that ESS's these days are configured to automatically detect any kind of scrambling going on, and alert security folks whenever a scrambled conversation is noticed. The rationale is that someone scrambling a conversation has something to hide, and the big government boys are interested in people who have things to hide. However, the aforementioned pair on the phone would not be noticed by an ESS, since all they would be doing is setting up a normal modem conversation, and if they didn't mind slow communication they could be even more secure with an encryption scheme that sent two or three lines of "noise" for every character of genuine information being transferred. The noise could look very innocuous, say the transactions on a "legal" bulletin board, and thus not even appear to be hiding anything.

By the way, those are the best possible secret codes, the kind that do not appear to be anything out of the ordinary and thus are not even thought to be codes at all! Another possibility is to send information in the form of the time delays between each character transmitted. That means that someone "listening in" on a digital conversation by having the data printed out would miss out on the entire message, since his printer would only record the characters sent, which in this instance are utterly unimportant. By the way, monitoring of a computer conversation may not be considered wiretapping since the statutes concerned can be narrowly interpreted to cover only audio taping of a conversation, not digital eavesdropping.

Informed as Hell

MANY PARTS OF "PUZZLE PALACE" BY JAMES BAMFORD SO INTO DETAIL ABOUT THE FORMS OF CRYPTOGRAPHY USED TODAY BY THE NATIONAL SECURITY AGENCY, WHICH INCIDENTALLY HAS EXPRESSED A STRONG INTEREST IN SUBSCRIBING TO US. WE HOPE THEY WILL CONTRIBUTE MANY FINE ARTICLES.

DEAR 2600:

Does 2400 baud work on standard Bell lines?

YES, 2400 BAUD IS ACTUALLY 4 BITS AT A TIME AT 600 BAUD. AND BELL LINES CAN HANDLE THAT.

DEAR 2600:

If I want to go trashing, am I forced to just attack my Central Office?

THERE ARE LOTS OF GOOD PLACES TO TRASH BESIDES PHONE COMPANIES. LOOK IN THE PHONE BOOK UNDER SOFTWARE COMPANIES, PHONE EQUIPMENT, COMPUTER EQUIPMENT, ELECTRONIC EQUIPMENT, OR LOOK AT RADIO SHACKS, OR GTE, MCI, OR YOUR LOCAL CABLE COMPANY. YOU WILL FIND LOADS OF THINGS, LIKE FREE TELEPHONES, FLOPPIES, ETC.

all kinds of letters

The 2600 Information Bureau

HOSTS BY LOCATION 27-Sep-84

STATE/COUNTRY HOST NAME	HOST ADDRESS	SITE ADDRESS
ALABAMA		
ANNIS-MIL-TAC	26.2.0.113	USASC - Anniston
GUNTER-ADAM	26.1.0.13	Air Force Data Systems
GUNTER-TAC	26.2.0.13	Air Force Data Systems
MICOM-TAC	26.2.0.41	Army Missile Command
MICOM-TEST	26.1.0.41	Army Missile Command
APO		
FRANKFURT-MIL-TAC	26.0.0.116	Defense Communications Agency
ARIZONA		
YUMA-DW	26.3.0.75	Army Yuma Proving Ground
YUMA-TAC	26.2.0.75	Army Yuma Proving Ground
CALIFORNIA, Northern		
A-LNI-GRI-01	10.7.0.51	GRI International
ALGA-UNIX	10.2.0.56	Advanced Information
AMELIA-EC	26.4.0.16	NAWA
AMES-NAS-DW	26.4.0.16	NASA
AMES-TAC	26.1.0.16	NAWA
AMES-VMSB	26.3.0.16	NASA
AMOS-SCOURE	26.4.0.33	Navy Fleet Numerical
NEUTREL	10.3.0.32	Kentrel Institute
LBL	26.0.0.24	University of California
LBL-CRAY	26.1.0.24	University of California
LBL-MILNET-DW	10.0.0.48	Lawrence Berkeley
LLL-CRG	26.3.0.21	University of California
LLL-MFE	26.1.0.21	University of California
LLL-TIB	26.0.0.21	University of California
LLL-TDIVISION	26.2.0.21	University of California
MPS	26.0.0.33	Naval Postgraduate School
MPS-TAC	26.2.0.33	Naval Postgraduate School
OFFICE-1	26.0.0.43	Tymshare, Inc.
OFFICE-10	26.1.0.43	Tymshare, Inc.
OFFICE-15	26.1.0.43	Tymshare, Inc.
OFFICE-2	26.2.0.43	Tymshare, Inc.
OFFICE-3	26.3.0.43	Tymshare, Inc.
OFFICE-7	26.3.0.43	Tymshare, Inc.
OFFICE-8	26.0.0.43	Tymshare, Inc.
PARC-MAIL	10.0.0.32	Xerox Corporation
PARC-VAX1	10.1.0.32	Xerox Corporation
RIACS-DW	26.6.0.16	Research Institute for
RIACS-ICARUS	26.4.0.16	Research Institute for
SU-A	26.1.0.73	University of California
SU-B	26.2.0.95	University of California
SU-B-DW	26.2.0.90	University of California
SU-C	26.3.0.95	University of California
SRI-AI	10.4.0.2	SRI International
SRI-CSL-TOPAZ-DW	10.1.0.107	SRI International
SRI-CSL	10.2.0.2	SRI International
SRI-FA	26.4.0.73	SRI International
SRI-DW	10.5.0.51	SRI International
SRI-IU	10.8.0.2	SRI International
SRI-KL	10.1.0.2	SRI International
SRI-MIL-TAC	26.3.0.73	SRI International
SRI-MILNET-DW	10.4.0.51	SRI International
SRI-NIC	10.0.0.51	SRI International
SRI-PR-SRI	10.1.0.51	SRI International
SRI-PR-VAX	10.3.0.51	SRI International
SRI-PR-VAX3	10.0.0.107	SRI International
SRI-SPAM-TEST	10.2.0.107	SRI International
SRI-SPAM	10.0.0.2	SRI International
SRI-TAC	10.3.0.2	SRI International
SRI-UNIX	10.2.0.51	SRI International
SRI-WAAF	26.1.0.73	SRI International
STANFORD-GATEWAY	10.1.0.11	Stanford University
SU-AI	10.0.0.11	Stanford University
SU-SCORE	10.3.0.11	Stanford University
SU-TAC	10.2.0.11	Stanford University
SUMEX-AIM	10.0.0.51	Stanford University Medical
UCB-ARPA	10.0.0.78	University of California
UCB-VAX	10.2.0.78	University of California
USGS3-TAC	26.1.0.70	U.S. Geological Survey
USGS3-VAX	26.0.0.70	U.S. Geological Survey
XEROX	10.2.0.32	Xerox Corporation
CALIFORNIA, Southern		
AGC	26.6.0.45	Advanced Computer
ACCAT-TAC	26.2.0.35	Naval Ocean Systems Center
ADA-VAX	26.2.0.103	USC
AERONET-DW	26.8.0.65	The Aerospace Corporation
AEROSPACE	26.2.0.65	The Aerospace Corporation
AFSC-SD	26.8.0.65	Air Force Systems Command
AFSC-SD-TAC	26.1.0.65	Air Force Systems Command
CIT-20	10.8.0.54	CALTECH
CIT-CS-DW	10.1.0.54	CALTECH
CIT-VAX	10.1.0.54	CALTECH
EDWARDS-2060	26.1.0.39	Edwards Air Force Base
EDWARDS-VAX	26.0.0.39	Edwards Air Force Base
ISI-GATEWAY	10.3.0.27	USC
ISI-HOSGOBLIN	10.1.0.52	USC
ISI-MOON-DW	10.1.0.52	USC
ISI-MILNET-DW	10.2.0.22	USC
ISI-PONG	10.1.0.27	USC
ISI-POAT-10	10.3.0.22	USC
ISI-SPEECH1	10.0.0.22	USC
ISI-VAX4	10.2.0.27	USC
JPL-VLSI	10.3.0.54	Jet Propulsion Laboratory
LOGICON	26.2.0.3	Logicon, Inc.
MARTIN-ED	26.3.0.45	Martin Marietta Corporation
NOSC	26.0.0.3	Naval Ocean Systems Center
NOSC-F4	26.4.0.35	Naval Ocean Systems Center
NOSC-DW	26.0.0.3	Naval Ocean Systems Center
NOSC-SECURE2	26.0.0.38	Naval Ocean Systems Center
NOSC-SECURE3	26.1.0.35	Naval Ocean Systems Center
NOSC-TECR	26.1.0.38	Naval Ocean Systems Center
NPRDC	26.1.0.3	Naval Personnel Research
NPRDC-DW	26.1.0.3	Naval Personnel Research
NTEC-TADDEN-001	26.1.0.3	Sperry Technical Services
NWC-3607	26.1.0.45	Naval Weapons Center
NWC-3607A	26.0.0.85	Naval Weapons Center
NWC-3878	26.2.0.85	Naval Weapons Center
NWC-TAC	26.2.0.85	Naval Weapons Center
RAND-ARPA-TAC	10.2.0.7	The Rand Corporation
RAND-UNIX	10.3.0.7	The Rand Corporation
RAND2-MIL-TAC	10.0.0.7	The Rand Corporation
UCLA-AIS	10.3.0.1	University of California
UCLA-CCN	10.1.0.1	University of California
UCLA-LOCUS	10.2.0.1	University of California
UCLA-TEST	10.0.0.1	University of California
USC-ECL	10.3.0.121	USC
USC-ECLB	10.0.0.23	USC
USC-ECLC	10.1.0.121	USC
USC-ISI	26.3.0.103	USC
USC-ISIB	10.3.0.52	USC
USC-ISIC	10.0.0.72	USC
USC-ISID	10.0.0.27	USC
USC-ISIE	26.1.0.103	USC
USC-ISIF	10.2.0.52	USC
USC-TAC	10.2.0.23	USC
COLORADO		
USGS2-MULTICS	26.0.0.49	U.S. Geological Survey
VMMM3-TAC	26.1.0.49	U.S. Geological Survey
CONNECTICUT		
NUWC	26.3.0.42	Naval Underwater Systems
YALE	10.2.0.9	Yale University
YALE-DW	10.3.0.9	Yale University
DELAWARE		
UDEL-EE	10.3.0.94	University of Delaware
UDEL-DW	10.0.0.96	University of Delaware
UUNL-DELAY	10.0.0.94	University of Delaware
ENGLAND		
NIMF-LON-EM	24.0.0.7	CINCUSNAVEUR
NIMET-LON-TAC	24.1.0.7	CINCUSNAVEUR
FLORIDA		
AFSC-AD	26.0.0.53	Air Force Armament Division
AFSC-AD-TAC	26.3.0.53	Air Force Armament Division
EGLIN-VAX	26.6.0.53	Eglin Air Force Base
JAXL-MIL-TAC	26.4.0.110	Navy Regional Data
MARTIN	26.3.0.53	Martin Marietta Corporation
MARTIN-D	26.1.0.44	Martin Marietta Corporation
NCSC	26.4.0.53	Naval Coastal Systems Center
GEORGIA		
CUMBER-FORCECOM	26.4.0.44	Forces Command
LOWER-FT8ILLH	26.0.0.64	U.S. Army
ROBINS-TAC	26.2.0.44	Warner-Robins ALC/MMECOM
ROBINS-UNIX	26.3.0.64	Warner-Robins ALC/MMECOM
GERMANY		
SCA-EUR	24.3.0.2	SCA Europe
MILNET-BRM-TAC	24.1.0.5	MILNET Installation
MILNET-GNL-TAC	24.1.0.4	SCA Europe
MILNET-GBL-EM	24.0.0.1	U.S. Army Camp King
MILNET-GNL-TAC	24.1.0.1	U.S. Army Camp King
MILNET-RAM-TAC	24.1.0.3	U.S. Air Force
MILNET-VHM-EM	24.2.0.2	SCA Europe
MILNET-VHM-TAC	24.1.0.2	SCA Europe
PATCH	26.6.0.3	Headquarters, U.S.E.COM
SECKENHEIM-EMH	26.4.0.116	Army Material Development
HAWAII		
CINCPAC-TAC	26.2.0.36	Commander in Chief Pacific
HAWAII-EMH	26.1.0.36	DCS Technical Control
ILLINOIS		
AFSC-1	26.4.0.118	Air Force Communications
AFSC-2	26.5.0.118	Air Force Communications
AFSC-3	26.6.0.118	Air Force Communications
AFSC-4	26.7.0.118	Air Force Communications
ANL-MCS	26.1.0.35	Argonne National Laboratory
COMPION-VMS	26.2.0.55	Gould Software Division
HQUTT-TAC	26.1.0.39	Air Force Communications
SCOTT2-MIL-TAC	26.0.0.110	Air Force Communications
INDIANA		
PURDUE-CS-DW	10.2.0.37	Purdue University
PURDUE-EE5	10.2.0.98	Purdue University
ITALY		
CPO	24.0.0.8	NTCC
MILNET-CPO-TAC	24.1.0.8	Naval Tele- [illegible]cations
MILNET-NSW-TAC	24.1.0.9	NATO Naval [illegible] Field
KOREA		
KOREA-EMH	26.0.0.117	AUTODIN Switching Center
KOREA-TAC	26.2.0.117	AUTODIN Switching Center
NORL-MIL-TAC	26.2.0.109	Navy Regional Data
LOUISIANA		
NAVCOMSLA-01100	26.3.0.109	Navy Regional Data
MARYLAND		
APG-1	26.1.0.29	Test and Evaluation Command
APG-2	26.6.0.29	Aberdeen Proving Ground
APG-3	26.4.0.29	Aberdeen Proving Ground
BRL	26.0.0.29	Army Armament Research
BRL-GATEWAY	26.3.0.29	Army Armament, Munitions
BRL-GATEWAY2	26.0.0.29	Army Armament Research
BRL-TAC	26.2.0.29	Army Armament Research
COINS-GATEWAY	26.1.0.87	National Security Agency
DAVID-TAC	26.2.0.91	David Taylor Naval Ship
DTNSRDC-DW	26.3.0.91	David Taylor Naval Ship
DTRC	26.3.0.91	David Taylor Naval Ship
MARYLAND	26.4.0.57	University of Maryland
MARYLAND-DW	26.2.0.57	University of Maryland
NRL-CCN	26.1.0.83	David Taylor Naval Ship
NBS-AMRF	26.6.0.17	National Bureau of Standards
NBS-EDC	26.1.0.17	National Bureau of Standards
NBS-SEC	26.7.0.17	National Bureau of Standards
NCHO	26.0.0.81	David Taylor Naval Ship
NLM-DW	26.0.0.88	National Institutes of Health
NLM-MCS	26.0.0.80	National Institutes of Health
NRRARCOA-DW	26.3.0.81	David Taylor Naval Ship
NSWC-WO	26.0.0.102	Naval Surface Weapons Center
PAX-RV-TAC	26.3.0.97	Naval Electronics Systems
PAXRV-NES	26.2.0.97	Naval Electronics Systems
TYCHO	26.0.0.37	National Security Agency
MASSACHUSETTS		
A-LNI-DDN-01	10.6.0.63	DDN Communications
AFCRL	26.1.0.46	Air Force Geophysics
AFGL-TAC	26.2.0.46	Air Force Geophysics
ARPANET-MC	10.5.0.80	BBN Communications
BBN-ARPA-TAC	10.1.0.63	Bolt Beranek and Newman Inc.
BBN-CLIO	10.0.0.3	Bolt Beranek and Newman Inc.
DDN-CRONUS-DN	10.6.0.92	Bolt Beranek and Newman Inc.
BBN-PJACKA-DW	10.2.0.3	Bolt Beranek and Newman Inc.
DDN-MIL-TAC	26.0.0.40	Bolt Beranek and Newman Inc.

BBN-MILNET-GW	10.3.0.3	BBN Communications
BBN-MINET-A-GW	26.1.0.40	BBN Communications
BBN-NET-GATEWAY	10.4.0.62	Bolt Beranek and Newman Inc.
BBN-PR-GW	10.4.0.3	Bolt Beranek and Newman Inc.
BBN-PR-STATION-1	10.7.0.8	Bolt Beranek and Newman Inc.
BBN-PRAT-IP	10.4.0.43	Bolt Beranek and Newman Inc.
BBN-RGW	VA.3.0.72	Bolt Beranek and Newman Inc.
BBN-TAFFO-GW	10.0.0.63	Bolt Beranek and Newman Inc.
BBN-UNIX	10.0.0.62	Bolt Beranek and Newman Inc.
BBN-VAN-GW	10.0.0.63	Bolt Beranek and Newman Inc.
BBN-VAN	10.1.0.62	Bolt Beranek and Newman Inc.
BBN-433-GW	10.0.0.44	BBN Communications
BBN-433-TEST1	10.3.0.77	BBN Communications
BBN-433-TEST4	10.4.0.77	BBN Communications
BBNA	10.3.0.5	Bolt Beranek and Newman Inc.
BBNCCP	10.3.0.44	Bolt Beranek and Newman Inc.
BBNG	10.1.0.5	Bolt Beranek and Newman Inc.
CCA-GAC	30.3.0.31	Computer Corporation of Amer.
CCA-UNIX	30.0.0.31	Computer Corporation of Amer.
CCA-VMS	30.1.0.31	Computer Corporation of Amer.
CISL-HVC-MULT	10.3.0.31	Honeywell Information Systems
CSNET-FDN-GW	10.4.0.5	Bolt Beranek and Newman Inc.
CSNET-RELAY	10.4.0.5	Bolt Beranek and Newman Inc.
CSNET-SH	10.7.0.52	Bolt Beranek and Newman Inc.
DDN2	26.2.0.72	Bolt Beranek and Newman Inc.
DEC-HUDSON	16.2.0.79	Digital Equipment Corporation
DEC-MARLBORO	16.1.0.79	Digital Equipment Corporation
DNET-TOPS20	16.0.0.79	Digital Equipment Corporation
HARVARD	10.0.0.9	Harvard University
HARVARD-GW	10.0.0.9	Harvard University
LL	18.0.0.18	MIT
LL-EH	10.4.0.10	MIT
LL-GW	10.8.0.18	MIT
LL-PRAT-IP	10.10.0.10	MIT
LL-SAT	10.4.0.10	MIT
LL-VLSI	10.1.0.10	MIT
LS-GW	10.2.0.10	MIT
MINET-TEST-EN	26.0.0.11	Movements Information Network
MIT-AI	10.2.0.4	MIT
MIT-GW	18.0.0.77	MIT
MIT-MC	10.3.0.44	MIT
MIT-ML	10.3.0.4	MIT
NET-MULTICS	10.0.0.4	MIT
NET-TAC	10.2.0.77	MIT
NLT-TOTOW	10.2.0.44	MIT
NET-XX	10.0.0.44	MIT
MITRE-BEDFORD	26.3.0.66	MITRE Corporation
TWPL	26.9.0.82	Bolt Beranek and Newman Inc.
TEST-HOSTS-225	10.3.0.99	BBN Communications
VAC-225	10.2.0.99	BBN Communications
MINNESOTA		
HI-MULTICS	10.3.0.74	Honeywell, Inc.
MISSOURI		
ALHDA-1	26.1.0.61	Automated Logistics
MIL-HUNTI	26.0.0.43	Army Aviation Systems Command
OTL-HOOTZ	26.0.0.112	Army Aviation Systems Command
SYLA-IAC	26.2.0.43	Army Information Systems
NEBRASKA		
DAC-ARPA-IAC	10.1.0.60	Strategic Air Command/ADXCC
DAC-GATEWAY	10.3.0.60	Strategic Air Command (SAC)
DAC-GW-2	10.5.0.60	Headquarters, SAC
DAC-MILNET-GW	10.2.0.60	SAC Command (SAC)
DAC-STATION	10.4.0.60	Headquarters, SAC
DACS-MIL-IAC	26.1.0.105	SAC Command/ADXCC
DACS-MIL-IAC	26.7.0.105	Headquarters, SAC
NEW HAMPSHIRE		
MITRE-JASON-HH2	26.0.0.92	Army Federal Systems
NEW JERSEY		
ARDC	26.1.0.45	Army Armament Research
ARDC-IAC	26.0.0.45	Army Armament Research
CECOM-1	26.3.0.40	Army Communications
CECOM-2	26.0.0.40	Army Communications
CORADCOM-IAC	26.1.0.40	Army Communications
CORADCOM2-IAC	26.2.0.40	Army Communications
MONMOUTH-ARPA	26.4.0.40	U.S. Army Communications
RUTGERS	10.1.0.87	Rutgers University
RUTGERS-GW	10.1.0.87	Rutgers University
TACTNET-GW	26.5.0.40	Army Communications
NEW MEXICO		
AFWL	26.1.0.48	Air Force Weapons Laboratory
AFWL-IAC	26.2.0.48	Air Force Weapons Laboratory
LANL	26.0.0.90	Los Alamos National
SANDIA	28.0.0.47	Sandia National Laboratories
SIMTEL20	26.0.0.74	White Sands Missile Range
WSMR-NET-GW	26.2.0.74	White Sands Missile Range
WSMR-IAC	26.4.0.74	White Sands Missile Range
WSMR01	26.1.0.74	White Sands Missile Range
NEW YORK		
BNL	26.1.0.50	Brookhaven National
COLUMBIA	10.0.0.89	Columbia University
COLUMBIA-30	30.0.0.89	Columbia University
COLUMBIA-GW	10.3.0.89	Columbia University
CORNELL	39.3.0.76	Cornell University
CORNELL-GW	10.3.0.76	Cornell University
GE-CRD	74.4.0.10	GE Corporate Research
NYU	26.0.0.50	New York University
NYU-GW	26.0.0.50	New York University
RADC-ARPA-IAC	10.0.0.117	Rome Air Development Center
RADC-LONEX	26.5.0.38	Rome Air Development Center
RADC-MULTICS	26.0.0.18	Rome Air Development Center
RADC-TAC	26.2.0.38	Rome Air Development Center
RADC-TOPS20	10.7.0.119	Rome Air Development Center
ROCHESTER	10.0.0.15	University of Rochester
UR-CS-GW	10.0.0.15	University of Rochester
NORTH CAROLINA		
BRAGG-ARPA-IAC	10.2.0.38	Chief, ADDB Experimental
BRAGG-PR-GW1	10.0.0.38	Chief, ADDB Experimental
BRAGG-PR-GW2	10.3.0.38	U.S. Army Airborne Board
BRAGG-SEA1	10.1.0.38	Chief, ADDB Experimental
OHIO		
CODNET2	26.0.0.47	Headquarters, Air Force
HFAFB-AF11A	26.5.0.47	Wright-Patterson Air Force
WPAFB-AFWAL	26.1.0.47	Air Force Wright
HFAFB-INFO1	26.3.0.47	Wright-Patterson Air Force
WPAFB-JALCF	26.4.0.47	Wright-Patterson Air Force
WPAFB-TAC	26.9.0.87	Aeronautical Systems
OKLAHOMA		
TAMINN-HILL-IG	26.1.0.71	Headquarters, Department of
TINKER-HIL-TAC	26.2.0.71	Tinker Air Force Base
PENNSYLVANIA		
CDA-POPOL	26.1.0.114	Army Material Development
CMU-CB-A	30.1.0.14	Carnegie-Mellon University
CMU-CB-B	26.7.0.47	Carnegie-Mellon University
CMU-CB-C	30.2.0.18	Carnegie-Mellon University
CMU-GATEWAY	30.2.0.14	Carnegie-Mellon University
LBBA-DB1	26.1.0.88	Letterkenny Army Depot
NADC	26.9.0.24	Naval Air Development Center
NCAD-MIL-TAC	26.7.0.118	New Cumberland Army Depot
NCADZ-MIL-TAC	26.5.0.114	New Cumberland Army Depot
WHARTON-10	10.1.0.96	University of Pennsylvania
RHODE ISLAND		
NAVDAF-NEWPORT	26.4.0.72	Naval Data Automation
NUSC-ADA	26.1.0.92	Naval Underwater Systems
NUSC-NPT	26.3.0.92	Naval Underwater Systems
SCOTLAND		
MINET-MLH-TAC	24.1.0.13	NAVACTS
TENNESSEE		
ORNL-MSR	26.3.0.43	Oak Ridge National Laboratory
TEXAS		
A-LMI-COL-02	10.4.0.44	Rockwell International
AFAFC-1	26.0.0.102	Headquarters, Air Force
AFMPC-2	26.1.0.30	Headquarters, Air Force
BROOKS-AFB-TAC	26.0.0.30	Air Force Systems Command
COLLINS-GW	10.1.0.46	Rockwell International
COLLINS-PR	30.0.0.46	Rockwell International
COLLINS-TAC	30.2.0.46	Rockwell International
IBMLRA-PTBL(83	26.4.0.74	U.S. Army
UT-NSF	30.0.0.62	University of Texas
UT-SALLY	30.2.0.62	University of Texas at Austin
UTEXAS-20	30.1.0.62	University of Texas
THE NETHERLANDS		
MINET-RDH-TAC	24.1.0.6	RPMS TTGE
UTAH		
DPG-1	26.1.0.120	Dugway Proving Ground
DUGWAY-MIL-TAC	26.0.0.120	Dugway Proving Ground
UTAH-20	10.3.0.4	University of Utah
UTAH-CS	10.0.0.4	University of Utah
UTAH-GATEWAY	10.0.0.4	University of Utah
UTAH-TAC	10.2.0.4	University of Utah
VIRGINIA		
ARI-HQ1	26.1.0.80	Army Research Institute
ARPA-MILNET-GW	10.2.0.38	Defense Advanced Research
ARPA-PMBJJ	26.3.0.106	Defense Advanced Research
ARPAI-MIL-TAC	26.1.0.106	Defense Advanced Research
ARPAT-MIL-TAC	26.2.0.106	Defense Advanced Research
ARPAI-IAC	10.0.0.26	Defense Advanced Research
ASPAW-CSC	26.2.0.9	Computer Sciences Corporation
CAC-GA	26.1.0.104	Computer Systems Command
CSS-GATEWAY	10.2.0.25	Teledyne Geotech
CSS-MILNS-GW	10.0.0.25	Teledyne Geotech
DARCOM-HQ	26.0.0.80	Army Material Development
DARCOM-IAC	26.2.0.80	Army Material Development
DARPA-GW	10.3.0.26	Center for Seismic Studies
DCEC-ARPA-IAC	10.2.0.20	Defense Communications
DCEC-GATEWAY	10.1.0.20	Defense Communications
DCEC-LNUN	26.4.0.104	Defense Communications
DCEC-LOUDS	26.1.0.104	Defense Communications
DCEC-MIL-TAC	26.2.0.104	Defense Communications
DCPC-MILNET-GW	10.7.0.20	Defense Communications
DCEC-PRAT	10.5.0.20	Defense Communications
DCEC-PRAT-IP	10.5.0.20	Defense Communications
DCEC-TAC	26.2.0.20	Defense Communications
DGW-GATEWAY	30.0.0.111	Linkabit Corporation
DDN-PHO-HIL-TAC	26.5.0.17	Defense Communications Agency
DURI	10.1.0.35	Bolt Beranek and Newman Inc.
EDN-UNIX	10.3.0.20	Defense Communications
ETL-AI	26.7.0.30	U.S. Army Engineer
HUEY-GW	26.1.0.17	MITRE Corporation
LWRIHN-CISC	26.2.0.67	Criminal Investigation
LWRIHO-DARCOM	26.4.0.67	U.S. Army Materiel
LWRIHO-TRADOC	26.4.0.84	Training and Doctrine Command
IPTU-HH	10.3.0.28	Defense Advanced Research
LOUIE-GW	10.3.0.111	MITRE Corporation
MITRE	26.0.0.17	MITRE Corporation
MITRE-GATEWAY	10.3.0.111	MITRE Corporation
MITRE-LAN	10.2.0.111	MITRE Corporation
MITRE-TAC	26.2.0.17	MITRE Corporation
NORFOLK-MILTAC	26.4.0.100	NAS Norfolk
NAVC-GW	26.0.0.44	Naval Surface Weapons Center
NSWC-DL	26.1.0.84	Naval Surface Weapons Center
NSWC-GW	26.3.0.84	Naval Surface Weapons Center
NSWC-TAC	26.7.0.84	Naval Surface Weapons Center
SETGWD	10.0.0.25	Teledyne Geotech
SDACC1B-GBC	26.3.0.94	Computer Sciences Corporation
USDACHQ	26.4.0.50	Headquarters SARCOM
WASHINGTON		
UW-VLSI	10.3.0.71	University of Washington
UW-VLSI-GW	10.3.0.71	University of Washington
WASHINGTON	10.0.0.71	University of Washington
WASHINGTON-IAC	10.2.0.71	University of Washington
WASHINGTON, D.C.		
AFSC-HQ	26.0.0.67	Air Force Systems
AFSC-HQ-IAC	26.1.0.67	Air Force Systems
DCA-EMS	26.5.0.104	Defense Communications Agency
LWRIHA-DAIG	26.1.0.94	Headquarters, Department of
NORDACWASH-DD1	26.7.0.8	Navy Regional Data
NBS-AL	26.3.0.19	National Bureau of Standards
NBS-UNIX	26.2.0.19	National Bureau of Standards
NBS-VMS	26.0.0.19	National Bureau of Standards
NRL	26.0.0.3	Naval Research Laboratory
NRL-AIC	26.1.0.9	Naval Research Laboratory
NRL-ARGTAN	26.4.0.9	Naval Research Laboratory
NRL-CSS	26.7.0.9	Naval Research Laboratory
NRL-CXM-GW	26.6.0.9	Naval Research Laboratory
NRL-TOPOLO	26.4.0.9	Naval Research Laboratory
PENTAGON-TAC	26.0.0.26	Air Force Data Services
WISCONSIN		
WISC-GATEWAY	10.0.0.44	University of Wisconsin

see page 1-31 for details on how to use this data